日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　２月　８日

出願番号
Application Number: 特願２０００－０２９９３８

出願人
Applicant (s): 有限会社イオネットワーク

CERTIFIED COPY OF PRIORITY DOCUMENT

２０００年１０月　６日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０８２２９８

【書類名】　特許願
【整理番号】　P200000-1
【あて先】　特許庁長官殿
【国際特許分類】　G09C　1/00
【発明者】
　【住所又は居所】　東京都大田区上池台１丁目５２番１０号　有限会社イオネットワーク内
　【氏名】　清本　尚一
【特許出願人】
　【識別番号】　598045276
　【氏名又は名称】　有限会社イオネットワーク
　【代表者】　清本　尚一
【代理人】
　【識別番号】　100083884
　【弁理士】
　【氏名又は名称】　田中　昭雄
【手数料の表示】
　【予納台帳番号】　034038
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報通信方法

【特許請求の範囲】

【請求項１】 通信当事者の特徴点により符号化された指紋情報を鍵として平文を暗号化し、且つ暗文を通信当事者の特徴点により符号化された指紋情報を鍵として復号化することを特徴とする通信方法。

【請求項2】 予め通信両当事者の特徴点により符号化された指紋情報を鍵管理システムに預け、通信両当事者の一方は特徴点により符号化された自己の指紋情報を鍵として暗号化したデータを上記鍵管理システムに送信し、鍵管理システムでは事前に預けられた一方の通信当事者の指紋情報を鍵として上記暗号化したデータを復号化し、次に他方の通信当事者から預かった指紋情報を鍵として復号化されたデータを暗号化したデータを他方の通信当事者に送信し、他方の通信当事者は特徴点より符号化された自己の情報を鍵として上記暗号化されたデータを復号化することを特徴とする通信方法。

【請求項3】 鍵管理システムに預けられた指紋情報と同じ指紋情報を別媒体に保持し、本人確認の必要時に出力して本人が確認された時点で、これを鍵として使用する請求項2記載の通信方法。

【発明の詳細な説明】

【０００１】

【発明が属する技術分野】

この発明は、インターネット等のさまざまな情報をやり取りされるコンピュータの通信網において、通信内容のセキュリティーを確保する情報通信の暗号化とこれを使用した情報通信方法に関するものである。

【０００２】

【従来の技術】

例えば、現行のインターネットでは、ネットワークを確立するプロトコル（接続手順）の中に、内容を隠す十分な仕組みが含まれていないために平文のままでデータのやり取りが行われており、通信の傍受、盗聴、偽造並びに乗っ取りに対して無防備といえる状態にある。

【０００３】

通信内容の安全性確保には、①通信内容の秘密保持（盗聴、偽造の可能性のある通信路上での安全確保）、②通信当事者の身元確認（送信、受信の非否認）の二つの不可欠である。

【０００４】

即ち、必ずしも転送路上での暗号化技術のみの議論だけでは済まされず、例えば強力な暗号化方式が開発されても、その機能を備え、しかも正しいアドレス（送り主と宛先の住所に相当）を持った通信端末（例えばパーソナル・コンピュータ）を使ったとしても、データを送信した人間が本人であったのか、逆に間違いなく目的の受信者が受信したのかが不問であれば安全で確実な通信は保証されない。

【０００５】

また、従来対称鍵暗号方式（互いに定めた同じ「鍵」と暗号化アルゴリズムを通信両当事者が交換、保持する）、公開鍵方式、対称鍵暗号方式（暗号化と復号化に別の「鍵」若しくは暗号化アルゴリズムを用いる）のような暗号化及び運用方式が開発され、一部で運用されている。

【０００６】

しかし、これらの暗号方式は基本的に通信路上でのセキュリティーの問題解決を目指すものであって、情報のやり取り全体の安全性の保証には不十分である。

【０００７】

一方、個人の認識情報として指紋が用いられ、これを「鍵」として暗号化する方法が提案されている（特開平9-274431号公報、特開平8-171535号公報、特開平11-282983号公報）。

【０００８】

【発明が解決しようとする課題】

しかし、この場合同一の指紋であっても指の置き方、指紋の状態（発汗、乾燥等）に依存し、得られる指紋画像には微妙なゆらぎを伴い、同一の指紋でも常に完全に同じ内容で再現されるとは限らないという欠点がある。

【０００９】

一方、読取られた指紋画像は、図３ に示すように、隆起した黒く見える連なりから構成される「隆線」と、隆線と隆線との間を構成する白く見える「谷線」とからなり、個々の指紋の特徴は、この「隆線」と「谷線」の「端点」と「分岐点」との配置及びその特性により識別されることが知られており、この「端点」と「分岐点」とを合せて「特徴点」と呼ばれるが、図４に示すように、「特徴点」により指紋情報を符号化すれば、上述のような指紋画像の微妙なゆらぎを防止することができる。

【００１０】

そこで、この発明では特徴点により符号化された指紋情報を利用して上記通信内容の秘密保持と通信当事者の身元確認の条件を同時に満たすような通信方法を開発することを目的とする。

【００１１】

【課題を解決するための手段】

このため、本願第1発明では通信当事者の特徴点により符号化された指紋情報を鍵として平文を暗号化し、且つ暗文を通信当事者の特徴点により符号化された指紋情報を鍵として復号化する通信方法を提案するものである。

【００１２】

即ち、この発明によれば特徴点により符号化された指紋情報を鍵として平文を暗号化し、暗文を復号化するため、上述のような指紋情報の微妙なゆらぎもなく、確実に通信内容の秘密保持と通信当事者の身元確認を同時に満足させることができる。

【００１３】

なお、この発明において指紋画像より特徴点を抽出する方法としては種々の方法を採用することができるが、従来の指紋画像の特徴点抽出手法は、画像を構成する階調を持った各画素を白又は黒の二値に置換える二値化を実行後、照合アルゴリズムの都合により、隆線（例えば黒画素列）又は谷線（例えば白画素列）のいずれか一方を１画素の太さになるまで細線化・芯線化し、更に指紋画像の全ての点を対象にして隆線又は谷線の方向と向きを算出し、上記指紋の芯線化情報と関係付けるといった複雑な手順による特徴点（端点又は分岐点）及び方向と向き

を決定する手法であった（コンピュータ画像処理：応用実践編３、総研出版株式会社、1992年10月10日発行）。

【００１４】

これに対して、先に本願出願人は指紋画像から隆線と谷線を定める手段と、この定められた隆線と谷線とから特徴点候補リストを作成する手段と、この特徴点候補リストに網羅された各特徴点を中心として予め定められた局所領域に着目し、この局所領域の境界上を横切る隆線と谷線の本数を求めることにより、この特徴点候補の方向と向き及び信頼係数を算出すると共に、偽の特徴点候補を排除して指紋の特徴点リストを作成する手段とからなる指紋画像の特徴点抽出方法を提案した（特願平10-356681号）。

【００１５】

この手法によれば、選ばれた特徴点の周囲の局所的な領域のみを処理することにより、指紋を特徴付ける特徴点の方向と向きの算出が可能となるため、処理過程を大幅に軽減することができる。

【００１６】

更に、上記指紋画像から隆線と谷線を定める手段として、指紋画像を三値化する方法、具体的には読取られた指紋画像を、従来の白と黒の他に、白か黒かの曖昧な場合の表現としての「灰色画素／領域」を新たに設定し、白、灰、黒の三つのレベルで、指紋画像の各画素を分類する、所謂三値化し、この三値化された画素のうち黒レベルを黒線化して例えば隆線を定め、白レベルを白線化して例えば谷線を定める方法を提案した（特願平10-356681号）。

【００１７】

この手法によれば、各特徴点の信頼係数を定義し、その算出、決定手段を確立することにより、簡便な手続により高い精度での指紋の特徴点抽出ができる。

【００１８】

本願の第2発明は予め通信両当事者の特徴点により符号化された指紋情報を鍵管理システム（信頼できる第三者）に預け、通信両当事者の一方は特徴点により符号化された自己の指紋情報を鍵として暗号化したデータを上記鍵管理システムに送信し、鍵管理システムでは事前に預けられた一方の通信当事者の指紋情報を鍵

として上記暗号化したデータを復号化し、次に他方の通信当事者から預かった指紋情報を鍵として復号化されたデータを暗号化したデータを他方の通信当事者に送信し、他方の通信当事者は特徴点より符号化された自己の情報を鍵として上記暗号化されたデータを復号化する通信方法を提案するものである。

【００１９】

即ち、本願の第1発明に係わる方法で暗号化された情報をやり取りする際に、この発明の方法によれば通信情報の安全性を確保できるのである。

【００２０】

更に、本願の第2発明において鍵管理システムに預けられた指紋情報と同じ指紋情報を別媒体に保持し、本人確認の必用時に出力して使用する方法を提案するものである。

【００２１】

即ち、図３からも予測されるように、同一の指紋であっても指の置き方、指紋の状態（発汗、乾燥等）に依存し、得られる指紋画像には微妙なゆらぎを伴い、このゆらぎが符号化された指紋情報にも微細な差を生じさせ、同じ特徴点抽出処理を経ても常に同じ内容の指紋情報が再現される訳ではないが、鍵管理システムに預けられた指紋情報と同じ指紋情報を別媒体に保持し、本人確認の必用時に出力して使用するようにすれば、通信内容を暗号化、復号化する際に、指紋情報のバラツキが通信内容に誤差として伝播する事態を回避することができる。

【００２２】

【実施例】

この発明に関するデータ通信処理手順を図１に沿って説明すると、図１は送信者（Ａ）が受信者（Ｂ）へある平文情報（｛Ｄ｝）を送信する場合を想定して、その処理手順を図示したものである。

【００２３】

送信者Ａが平文｛Ｄ｝を用意した後、「鍵管理システム」への送信を開始し（符号６参照）、「鍵管理システム」との通信が確立すると通信端末は、送信者Ａに対し例えば指紋による本人確認を要求する（符号7参照）。

【００２４】

本人認証は例えば特願平10-356681号に詳しく述べられているが、読取られた指紋画像（図1）から特徴点抽出処理により図2に示すように符号化された指紋情報（以下、単に「指紋情報」と呼ぶ）に置換えられる。

【００２５】

次に、送信者Aの「指紋情報」を鍵として平文〔D〕を暗号化するが（符号8参照）、上述の通り同一の指紋であっても指の置き方、指紋の状態により得られる指紋画像には微妙な差異が生じて、同一の指紋にも拘わらず「指紋情報」が常に完全に同じで再現されるとは限らず、一方鍵としての「指紋情報」に要求される確度は常に100％でなければならず、この符号7で示される工程と符号8で示される工程の隔たりを解決する一実施例を図２に示す。

【００２６】

図２は、送信者Ａと受信者Ｂが夫々の鍵となる「指紋情報」を予め格納して保持し、本人確認の必要時に指紋を用いて本人を確認し、本人が確認された時点で出力し、これを鍵となる「指紋情報」として使用する指紋情報格納・出力専用装置のブロック図であり、

これに従って説明すると、「指紋情報」記憶部25に送信者Ａと受信者Ｂが夫々の鍵となる「指紋情報」を予め格納して保持し、通信端末より中央処理装置21に本人確認要求が指示されると、中央処理装置21は指紋読取り部19を動作状態にし、送信者Aが自分の指紋をライブで押捺し、指紋画像を入力する。

【００２７】

そのライブ画像データは特徴抽出回路20に送られた結果を記憶バッファ23に送る。次に、中央処理装置21の指示により指紋照合演算回路23がこれに記録されているライブ指紋情報と「指紋情報」記憶部25に記録されている「指紋情報」とを照合し結果を中央処理装置21に通知する。

【００２８】

この照合結果で本人であることが確認されると、中央処理装置21は「指紋情報」記憶部25に指示し、データを「指紋情報」記憶部25から通信端末との入出力制御部22を介して通信端末に送る。

【００２９】

なお、図２中太線はデータの、細線は信号の伝送路を意味し、点線は通常は使用されず上記「鍵管理システム」へ初期登録時又は異常時にのみ使用されることを意味する。

【００３０】

即ち、通常は「指紋情報」記憶部25は書き換えられることの無い出力専用記憶回路であると共に、ライブ指紋の特徴データはこの装置外には出力されない。

【００３１】

図２に示す装置により、本人であることが確認された後に、送信者Aの「鍵管理システム」に登録した際の「指紋情報」を読み出し、これを鍵として平文｛D｝を暗号化し、暗文｛D｝に変換される（符号8参照）。

【００３２】

「指紋情報」を鍵として暗号化する最も単純な方法の一例としては、平文｛D｝と「指紋情報」とをビット単位で排他的論理和演算｛XOR演算、OpenDesign No. 14（1996）「集中特集 最新の暗号技術によるセキュリティの実現」（CQ出版株式会社）参照｝をおこなう方法等がある。なお、データ長の差は、一方を繰返し使用する等の方法で合せればよい。

【００３３】

この演算は、可逆であると共に、鍵が不明である限り破られることはない。勿論、鍵の内容は生体個々の指紋から抽出された情報であることから、この鍵の内容が他人の手に渡ることはない。

【００３４】

上述のように暗号化されて暗文｛D｝が送信されると（符号9参照）、「鍵管理システム」は暗文｛D｝受信後、鍵データベース12を検索し、事前に送信者Aから委託済みの指紋情報を用いて、受け取った暗文｛D｝を平文｛D’｝に復号化する（符号11参照）。

【００３５】

次に、鍵データベース12から受信者Bより委託された指紋情報を検索し、これを鍵として平文｛D’｝を暗号化し、この暗文｛D’｝を計算し保持する（符号13参照）。

【００３６】

一方、受信者Ｂが受信作業を開始し（符号14参照）、「鍵管理システム」との通信が確立すると、通信端末は受信者Ｂに対して図２に示される指紋情報格納・出力専用装置により本人であることの確認を要求する（符号15参照）。

【００３７】

ここで本人であることが確認された後に通信端末は「鍵管理システム」に暗文｛D'｝の送信要求を発行し、それを受信する（符号16参照）。

【００３８】

受信終了後、結果の状態信号を「鍵管理システム」に発行すると共に（符号17参照）、登録済みの受信者Ｂの「指紋情報」を鍵として受信した暗文｛D'｝を復号化し、元の平文｛D｝を受信者Ｂに伝える（符号18参照）。

【００３９】

この実施例によれば、インターネット等のさまざまな情報がやり取りされるコンピュータの通信網において、備えるべき①通信内容の第3者により盗聴、改竄と偽造、②データを送信した本人が後で送信事実とその内容を否認することを不可能にする、③データを受け取った受信者が内容を改竄したり、受け取った事実を否認することを不可能にする、④誰でもこの発明に基づく暗号化方式の有効性を確認することを可能にする等のセキュリティーを保証することができる。

【００４０】

【発明の効果】

以上要するに、この発明によれば特徴点により符号化された指紋情報を利用して上記通信内容の秘密保持と通信当事者の身元確認の条件を同時に満たす通信方式が可能となる。

【図面の簡単な説明】

【図１】 情報の送信者Ａが受信者Ｂへデータを送信する場合におけるこの発明による処理手順を図示した流れ図

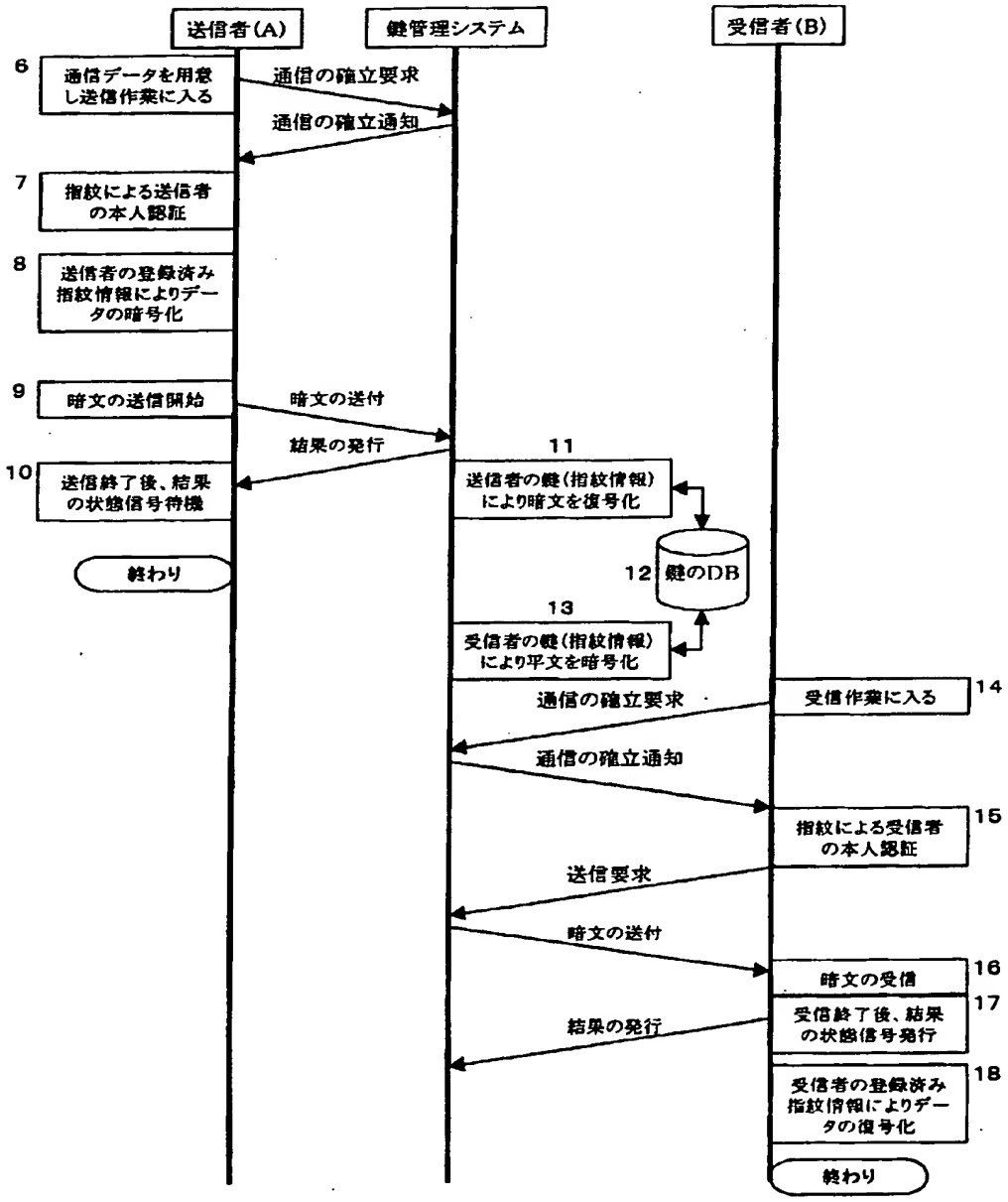
【図２】この発明で使用する指紋情報格納・出力専用装置のブロック図

【図3】 読取られた指紋画像の説明図

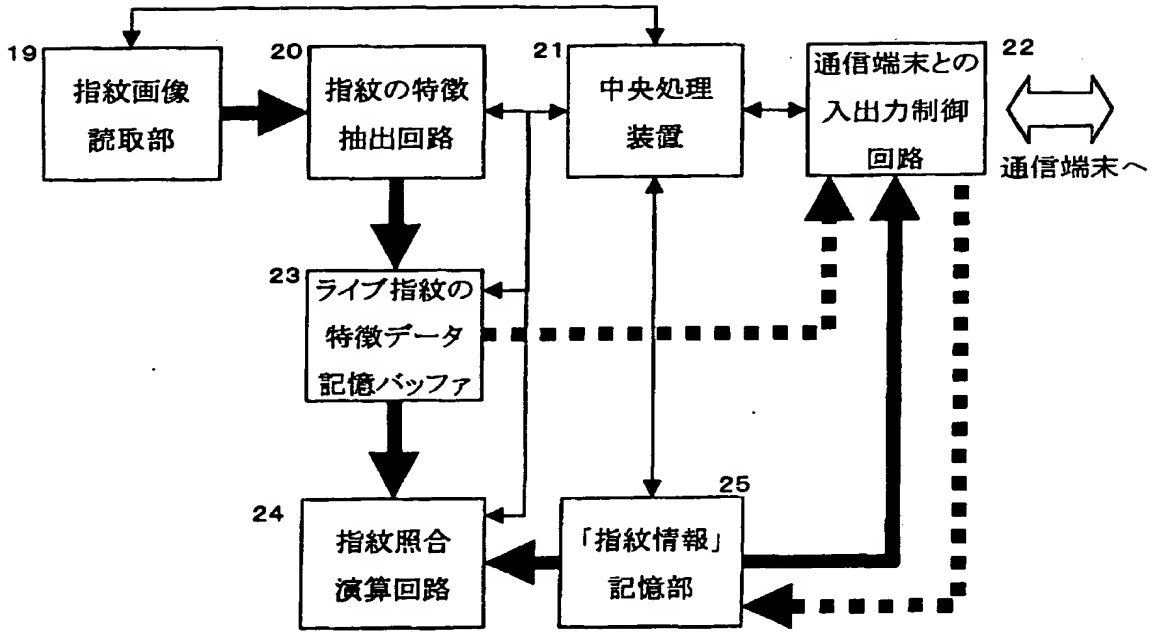
【図4】 特徴点により符号化された指紋情報図

【書類名】　　図面

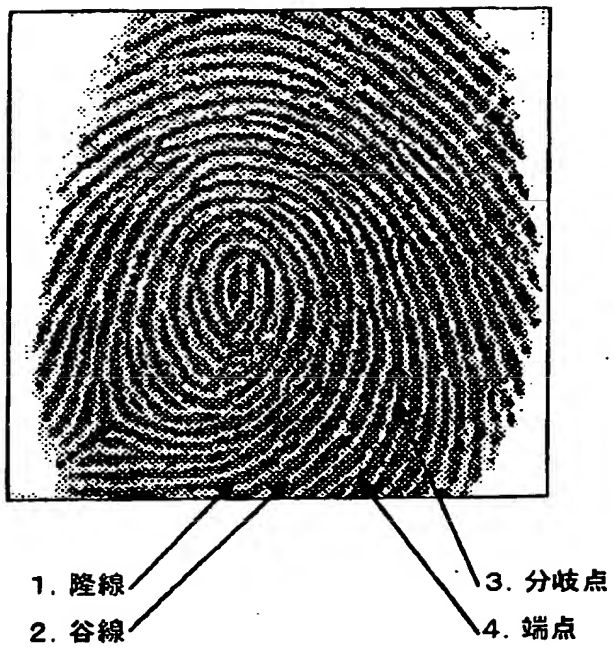
【図１】


送信者(A)
鍵管理システム
受信者(B)
6
通信データを用意し送信作業に入る
通信の確立要求
通信の確立通知
7
指紋による送信者の本人認証
8
送信者の登録済み指紋情報によりデータの暗号化
9
暗文の送信開始
暗文の送付
結果の発行
10
送信終了後、結果の状態信号待機
終わり
11
送信者の鍵(指紋情報)により暗文を復号化
12
鍵のDB
13
受信者の鍵(指紋情報)により平文を暗号化
通信の確立要求
受信作業に入る
14
通信の確立通知
指紋による受信者の本人認証
15
送信要求
暗文の送付
暗文の受信
16
結果の発行
受信終了後、結果の状態信号発行
17
受信者の登録済み指紋情報によりデータの復号化
18
終わり

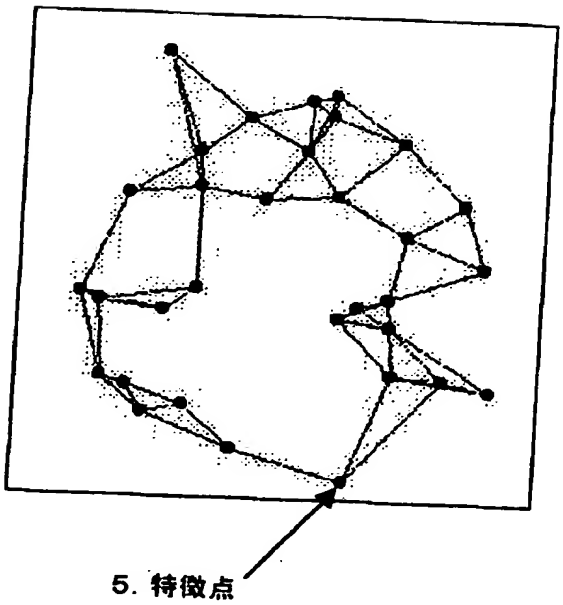
【図２】


19
指紋画像
読取部
20
指紋の特徴
抽出回路
21
中央処理
装置
通信端末との
入出力制御
回路
22
通信端末へ
23
ライブ指紋の
特徴データ
記憶バッファ
24
指紋照合
演算回路
25
「指紋情報」
記憶部

【図3】



【図4】



【書類名】　　要約書

【要約】

【課題】　特徴点により符号化された指紋情報を利用して上記通信内容の秘密保持と通信当事者の身元確認の条件を同時に満たすような通信方法を開発することを目的とする。

【解決手段】　予め通信両当事者の特徴点により符号化された指紋情報を鍵管理システム（信頼できる第三者）に預け、通信両当事者の一方は特徴点により符号化された自己の指紋情報を鍵として暗号化したデータを上記鍵管理システムに送信し、鍵管理システムでは事前に預けられた一方の通信当事者の指紋情報を鍵として上記暗号化したデータを復号化し、次に他方の通信当事者から預かった指紋情報を鍵として復号化されたデータを暗号化したデータを他方の通信当事者に送信し、他方の通信当事者は特徴点より符号化された自己の情報を鍵として上記暗号化されたデータを復号化する通信方法。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－０２９９３８
受付番号	５００００１３７２７２
書類名	特許願
担当官	第七担当上席　００９６
作成日	平成１２年　２月２３日

＜認定情報・付加情報＞

【提出日】	平成12年 2月 8日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔５９８０４５２７６〕

１．変更年月日　　１９９８年　４月　６日
［変更理由］　新規登録
住　所　東京都大田区上池台一丁目５２－１０
氏　名　有限会社イオネットワーク